## CLAIMS

1. A method for enforcing service policies over a network, said method implemented in a network device, comprising the steps of:

a. receiving authentication messages for a user at said network device;

b. determining user identifiers and service attributes associated with said user;

c. creating a user service policy entry in a user policy table for said identified user containing said service attributes;

d. consulting said user policy table to determine how to manage said user traffic subsequent to said user authentication messages; and

e. managing subsequent user traffic based on said consulting step.

2. A method for enforcing service policies over a network, as per claim 1, wherein said determining step includes monitoring and parsing said user authentication messages to obtain said user identity and attributes associated with said user.

3. A method for enforcing service policies over a network, as per claim 1, wherein said user policy table is located within said network device.

4. A method for enforcing service policies over a network, as per claim 1, wherein said network device offers internal network services comprising at least one of bandwidth management, access control or network usage statistics.

5. A method for enforcing service policies over a network, as per claim 1, wherein said authentication messages are using any of the Radius protocol or the LDAP protocol.

6. A method for enforcing service policies over a network, as per claim 1, wherein said network device functions in any one of, or a combination of, the following modes:

a. transparent mode, wherein the authentication messages in a provider network pass through the network device without any modification to the IP addresses and data of said authentication messages;

b. proxy mode, wherein the authentication messages in a provider network pass through the network device, said network device modifies IP addresses of said authentication messages without any modification to the data of said authentication messages; and

c. passive mode, wherein the authentication messages in a provider network are copied to the network device.

7. A method for managing network user traffic received by a network device, said network user traffic including at least a request for a server or service, said method comprising steps of:

a. identifying a user originating said network user traffic;

b. consulting a user policy table to locate a user service policy corresponding to said user; and

c. managing said network user traffic based on said consulting step by any one or more of the following:

i. forwarding network user traffic to a requested server,

ii. redirecting network user traffic to a server providing a same service as a requested server,

iii. sending network user traffic through filtering software before forwarding user traffic to a requested server,

iv. denying transmission of user traffic on the basis of access privileges,

v. counting or logging user traffic in order to provide network usage information,

or

vi. denying or delaying transmission of network user traffic on the basis of service level parameters.

8. A method for managing network user traffic received by a network device, as per claim 7, wherein said user policy table is filled according to information in user authentication messages.

9. A method for managing network user traffic received by a network device, as per claim 8, wherein authentication messages are using any of the Radius protocol or the LDAP protocol.

10. A method for managing network user traffic received by a network device, as per claim 7, wherein said network device offers internal network services comprising at least one of bandwidth management, access control or network usage statistics.

11. A method for managing network user traffic received by a network device, as per claim 7, wherein said network device functions in any one of the following modes:

a. transparent mode, wherein the authentication messages in a provider network pass through the network device without any modification to the IP addresses and data of said authentication messages;

b. proxy mode, wherein the authentication messages in a provider network pass through the network device, said network device modifies IP addresses of said authentication messages without any modification to the data of said authentication messages; and

c. passive mode, wherein the authentication messages in a provider network are copied to the network device.

12. A method for enforcing service policies over a network, said method implemented in a network device comprising steps of:

a. receiving authentication messages for a user at said network device;

b. determining user identifiers and service attributes associated with said user;

c. creating a user service policy entry in a user policy table for said identified user based on said service attributes;

d. consulting said user policy table to determine how to manage user traffic subsequent to said user authentication message; and

e. managing said subsequent user traffic including any one or more of the following:

i. forwarding user traffic to requested server,

ii. redirecting user traffic to a server providing same service as requested server,

iii. sending user traffic through filtering software before forwarding user traffic to requested server,

iv. denying transmission of user traffic on the basis of access privileges,

v. counting or logging user traffic in order to provide network usage information

or

vi. denying or delaying transmission of user traffic on the basis of service level parameters.

13. A method for enforcing service policies over a network, as per claim 12, wherein authentication messages are using any of the Radius protocol or the LDAP protocol.

14. A method for enforcing service policies over a network, as per claim 12, wherein said network device offers internal network services comprising at least one of bandwidth management, access control or network usage statistics.

15. A method for enforcing service policies over a network, as per claim 12, wherein said network device functions in any one of the following modes:

a. transparent mode, wherein the authentication messages in a provider network pass through the network device without any modification to the IP addresses and data of said authentication messages;

b. proxy mode, wherein the authentication messages in a provider network pass through the network device, said network device modifies IP addresses of said authentication messages without any modification to the data of said authentication messages; and

c. passive mode, wherein the authentication messages in a provider network are copied to the network device.

16. A system for enforcing service policies over a network comprising the following:

a user request-issuing device;

a service provider network over which user authentication messages and user traffic originated by said user request-issuing device is transmitted;

an authentication server to which said user request-issuing device attempts to connect and by which said user request-issuing device is authenticated and registered; and

a service policy director independent of said authentication server, enforcing a service policy for said user request-issuing device,

wherein said user request-issuing device may be included in at least a network access server of a service provider network or in a user network.

17. A system for enforcing service policies over a network, as per claim 16, wherein said service policy director includes a user policy table.

18. A system for enforcing service policies over a network, as per claim 17, wherein said user policy table includes user identifier information and service attribute information.

19. A system for enforcing service policies over a network, as per claim 18, wherein said user identifier information includes at least an Internet/intranet address.

20. A system for enforcing service policies over a network, as per claim 19, wherein said user identification information further includes any of username, session identification or Internet cookie.

21. A system for enforcing service policies over a network, as per claim 18, wherein said attribute information includes any one or more of the following: access privileges parameters, traffic logging mechanisms and user activity statistics entitlement parameters, security services entitlement parameters, or service quality level parameters.

22. A system for enforcing service policies over a network, as per claim 21, wherein said service quality level parameters include any one or more of the following: a bandwidth limit, a bandwidth guarantee, or a bandwidth priority.

23. A system for enforcing service policies over a network, as per claim 25, wherein said service attributes define services offered by said service policy director, said services

including any one or more of the following: classification of network user traffic, modification of network user traffic, forwarding of network user traffic, or logging of single network user traffic statistics.

24. A system for enforcing service policies over a network, as per claim 16, wherein said network device offers internal network services including at least one of bandwidth management, access control or network usage statistics.

25. A system for enforcing service policies over a network, as per claim 18, wherein a plurality of said service policy directors reside on a network.

26. A system for enforcing service policies over a network, as per claim 16, wherein said network device including said service policy director functioning in a transparent mode, wherein the authentication messages in a provider network pass through the network device without any modification to the IP addresses and data of said authentication messages.

27. A system for enforcing service policies over a network, as per claim 26, wherein said service policy director functioning in said transparent mode receives said user authentication request messages addressed to said authentication server and forwards said user authentication request messages to said authentication server.

28. A system for enforcing service policies over a network, as per claim 16, wherein said network device including said service policy director functioning in a proxy mode, wherein the authentication messages in a provider network pass through the network device, said network device modifies IP addresses of said authentication messages without any modification to the data of said authentication messages.

29. A system for enforcing service policies over a network, as per claim 28, wherein said service policy director functioning in said proxy mode receives said user authentication request messages addressed to said service policy director and forwards it to said authentication server.

30. A system for enforcing service policies over a network, as per claim 16, wherein said network device comprising said service policy director functioning in a passive mode, wherein the authentication messages in a provider network are copied to the network device.

31. A system for enforcing service policies over a network receiving user access request traffic, said system comprising a service policy director in any of the following configurations:

a user request-issuing device operatively connected a service policy director, said service policy director connected to an authentication server, and said authentication server being operatively connected to said user request-issuing device,

wherein said service policy director receives said user authentication request messages addressed to said authentication server and forwards said user authentication request messages to said authentication server;

a user request-issuing device operatively connected a service policy director, said service policy director being operatively connected to said user request-issuing device, and an authentication server being operatively connected to said service policy director, wherein said service policy director, receives said user authentication request messages and queries said authentication server; and

a user request-issuing device operatively connected to a service policy director, said service policy director receiving copied network user traffic, said copied network user traffic copied by a network device, and said user-request issuing device being operatively connected to said service policy director, the service policy director receives a copy of said user authentication request messages addressed to and destined for said authentication server.